UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,648	05/08/2001	Ricky Huang	002.0200.01	3593

22895	7590	09/08/2004

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER
BARQADLE, YASIN M

ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 09/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/851,648	HUANG ET AL.
	Examiner	**Art Unit**
	Yasin M Barqadle	2153

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _08 May 2001_.

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-30_ is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-30_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a) ☐ All   b) ☐ Some * c) ☐ None of:

       1. ☐ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____.

       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
     Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claims 1-30 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international applicat   ion by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-2, 4-6, 8-12, 14-18 and 20-21 are rejected under 35

U.S.C. 102(e) as being anticipated by Slivka et al USPN

(6256668).

As per claim 1, Slivka et al teach a system for providing Web-

based remote security application client administration in a

distributed computing environment (fig. 2 and fig. 7),

comprising:

a self-extracting configuration file containing an

executable configuration file (col. 15, lines 53-58) that is

self-extractable on a target client into an administered security

application [col. 13, lines 26-37];

an executable control embedded within an active

administration Web page [col. 13, lines 26-47 and col. 18, lines

53-67], the executable control being triggered upon each request

for the active Web page and causing dynamic Web content to be

generated therefrom [col. 13, lines 26-47];

a Web server (fig. 6, server 118) exporting a Web portal

comprising the active administration Web page to a browser

application (fig. 7, 146; col.13, lines 3-15 and abstract)

independent of a specific operating environment (col. 11, line 43

to col. 12, line 18) and interpreting the executable control to

facilitate copying of the self-extracting configuration file to

the target client [col. 13, lines 26-47 and col. 15, lines 1-35].

As per claim 2, Slivka et al teach the system according to Claim

1, further comprising:

the Web server (fig.3, 40 and fig. 6, 118) facilitating

copying of the self-extracting configuration file concurrently to

a plurality of target clients [col. 5, lines 15-46 and col. 15,

lines 1-35].

As per claim 4, Slivka et al teach the system according to Claim

1, further comprising:

the Web server monitoring the status of the copying of the

self-extracting configuration file to at least one target client

[col. 16, lines 1-38].

As per claim 5, Slivka et al teach the system according to Claim

1, further comprising:

the Web server reporting the status of security application

configuration on at least one target client [col.7, lines 39 to

col. 8, line 5].

As per claim 6, Slivka et al teach the system according to Claim

1, further comprising the self-extracting configuration file

performing at least one of an installation, configuration,

updating, and patching of the security application by executing

the executable configuration file [col. 13, lines 26-47].

As per claim 8, Slivka et al teach the system according to Claim 1, wherein the executable configuration file comprises at least one of a virus scanning, virus screening, active security, firewall, and VPN performance reporting application [col. 16, lines 1-38 and col. 17, lines 12-55].

As per claim 9, Slivka et al teach the system according to Claim 1, wherein the executable configuration file is a cabinet archival file [col. 15, lines 20-35].

As per claim 10, Slivka et al teach the system according to Claim 1, wherein the distributed computing environment is TCP/IP compliant [col. 6, lines 25-28].

As per claim 11, Slivka et al teach a method for providing Web-based remote security application client administration in a distributed computing environment (fig.3 and fig. 6), comprising:

storing a self-extracting configuration file containing an executable configuration file that is self-extractable on a target client into an administered security application [col. 13, lines 26-47 and col. 15, lines 1-35];

providing an executable control embedded within an active administration Web page, the executable control being triggered upon each request for the active Web page and causing dynamic Web content to be generated therefrom [col. 13, lines 26-47 and col. 18, lines 53-67. see abstract];

exporting a Web portal comprising the active administration
Web page to a browser application independent of a specific
operating environment (col. 11, line 43 to col. 12, line 18 and
(col.13, lines 3-15); and

interpreting the executable control to facilitate copying of
the self-extracting configuration file to the target client [col.
13, lines 26-47 and col. 15, lines 1-35].
As per claim 12, Slivka et al teach the method according to Claim
11, further comprising:

facilitating copying of the self-extracting configuration
file concurrently to a plurality of target clients [col. 5, lines
15-46 and col. 15, lines 1-35].

As per claim 14, Slivka et al teach the method according to Claim
11, further comprising:

monitoring the status of the copying of the self-extracting
configuration file to at least one target client [col. 16, lines
1-38].

As per claim 15, Slivka et al teach the method according to Claim
11, further comprising:

reporting the status of security application configuration
on at least one target client [col.7, lines 39 to col. 8, line
5].

As per claim 16, Slivka et al teach the method according to Claim
11, further comprising:

performing at least one of an installation, configuration,
updating, and patching of the security application by executing
the executable configuration file [col. 13, lines 26-47].

As per claim 17, Slivka et al teach the method according to Claim
11, wherein the executable configuration file comprises at least
one of a virus scanning, virus screening, active security,
firewall, and VPN performance reporting application [col. 13,
lines 26-47].

As per claim 18, Slivka et al teach the method according to Claim
11, wherein the executable configuration file is a cabinet
archival file [col. 16, lines 1-38 and col. 17, lines 12-55].

As per claim 20, Slivka et al teach the method according to Claim
11, wherein the distributed computing environment is TCP/p-
compliant [col. 6, lines 25-28].

As per claim 21, Slivka et al teach the computer-readable storage
medium holding code for performing the method according to Claim
11 [col. 4, lines 53-67].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms

the basis for all obviousness rejections set forth in this Office

action:

> (a) A patent may not be obtained though the invention is not identically
> disclosed or described as set forth in section 102 of this title, if the
> differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at
> the time the invention was made to a person having ordinary skill in the
> art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

Claims 3,7,13, 19 and 22-30 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Slivka et al USPN (6256668) in view of

Kraenzel et al USPN (6742026).

As per claim 22, Slivka et al teach a system for remotely

administering a client application using a Web-based portal in a

TCP/IP-compliant environment (fig.3, 40 and fig. 6, 118),

comprising:

storing an archival configuration file capable of self-

extracting on a target client into an executable configuration

file [col. 35-50];

an executable control into an active administration Web

page, the executable control being triggered upon each request

for the active Web page and causing dynamic Web content to be

generated therefrom [col. 13, lines 26-47 and col. 18, lines 53-67];

a Web server (fig.3, 40 and fig. 6, 118), serving the active administration Web page to a browser application to a requesting administrator (col. 11, line 43 to col. 12, line 18), comprising:

a transfer module interpreting the executable control upon successful credentialing to facilitate substantially concurrent copying of the self-extracting configuration file to at least one target client [col. 5, lines 15-46 and col. 15, lines 1-35].

Regarding claim 22, although Slivka et al shows substantial features of the claimed invention, he does not explicitly show a security module confirming credentials for requesting administrators against a list of authorized administrators. Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Slivka et al, as evidenced by Kraenzel et al USPN. (6742026).

In analogous art, Kraenzel et al whose invention is about a system for providing distributable runtime to services and application, disclose security module confirming credentials for requesting administrators against a list of authorized administrators [Col. 5, lines 39-46 and col. 10, lines 50-65]. Giving the teaching of Kraenzel et al, a person of ordinary skill in the art would have readily recognized the desirability and the advantage of modifying Slivka et al by employing the layered security module of Kraenzel et al because it allows the flexibility for controlling access to all or part of an

application so that users with the right credentials would be permitted to perform tasks based on their access lever of security.

As per claims 23 and 27, Slivka et al teach the invention, further comprising:

the Web server continuously monitoring the status of the copying of the self-extracting configuration file to the at least one target client [col. 7, lines 14-49]; and

the Web server generating a status event upon completion of the copying [col.7, lines 39 to col. 8, line 5].

As per claims 24 and 28, Slivka et al teach the invention, further comprising:

the Web server reporting the status of each application configuration on the at least one target client [col.7, lines 39 to col. 8, line 5].

As per claims 3 and 13, Kraenzel et al teach the invention, further comprising:

the Web server checking administrator credentials while exporting the Web portal against a list of authorized administrators [Col. 5, lines 39-46 and col. 10, lines 50-65].

As per claim 26, this claim has similar limitations as claim 22 above. Therefore, it is rejected with the same rationale.

As per claims 19, 25 and 29, Kraenzel et al teach the invention, wherein the active control is an Active X-compliant control [col. 9, lines 24-33].

As per claim 30, Slivka et al teach the computer-readable storage medium holding code for performing the method according to Claim 26 [col. 4, lines 53-67].
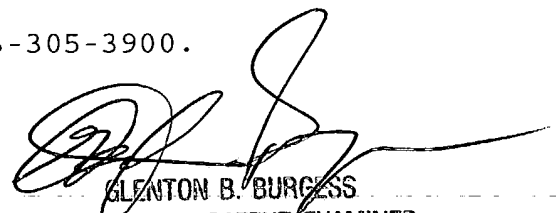
Conclusion

The prior made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yasin Barqadle whose telephone number is 703-305-5971. The examiner can normally be reached on 9:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess can be reached on 703-305-4792. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9306 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Yasin Barqadle

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100